

**PacketSight 1.0**

# **PacketSight 1.0**

## **Information Source Module Guide**

## Notices

This publication and the features described in it are subject to change without notice. While reasonable precautions have been taken in the preparation of the text, XACCT Technologies Ltd. and its subsidiaries ("XACCT") assume no responsibility or liability for any errors or omissions relating to the information or recommendations contained in this publication. The XACCT software products (the "Products") described in this publication are furnished expressly subject to the XACCT End-user License Agreement (the "Agreement"), which may be modified from time to time, and may be used or copied only in accordance with the terms and conditions set forth in the Agreement. The Product or components thereof may be protected by one or more US patents, foreign patents, pending applications, or national and international copyright laws. The Agreement contains, inter alia, limitations of liability and limited warranties. Please refer to the Agreement prior to installing or using the Product. THE USE OF THE PRODUCT IS EXPRESSLY SUBJECT TO THE TERMS AND CONDITIONS OF THE AGREEMENT.

XACCT, XACCT*usage*, XACCT Detail Record (XDR) and the XACCT logo are trademarks or registered trademarks of XACCT Technologies Ltd. All other products or services mentioned herein are trademarks or registered trademarks of their respective owners. The XACCT product includes software developed by the Cryptix Development Team (<http://www.systemics.com/docs/cryptix/>).

Copyright © XACCT Technologies Ltd. All rights reserved.

XACCT Technologies, Inc.  
USA  
Tel: 408-654-9900  
Fax: 408-654-9904

XACCT TEchnologies Ltd.  
Israel  
Tel: 972-3-5764111  
Fax: 972-3-6123737

URL: [www.xacct.com](http://www.xacct.com)

Email: [info@xacct.com](mailto:info@xacct.com)

May 25, 2001

# Contents

Overview .....	5
Connecting With XACCTusage.....	6
Features of the PacketSight ISM.....	7
Information Source Setup.....	7
Installing the PacketSight ISM.....	8
Adding a PacketSight ISM to the XACCTusage Configuration.....	10
Initial Setup.....	13
Using XML to Configure the PacketSight ISM .....	14
Data Collecting Elements .....	15
Event Elements .....	16
Domain Elements.....	17
Probe Attributes .....	18
Timestamps Group.....	18
Services Group.....	18
Protocols .....	19
HTTP Related Fields.....	19
EMAIL Related Fields .....	19
FTP Related Fields.....	19
RTSP Related Fields .....	20
NNTP Related Fields .....	20
Configuring Performance Metrics .....	21
Count Performance Metrics .....	21
Full Performance Metrics.....	22
PacketSight ISM Output Fields.....	23
Performance Metrics.....	23
Jitter Metrics .....	24
Exchange Response Metrics .....	25
Application Response Metrics .....	27
Connection Metrics .....	29
Connection Window Metrics .....	30
Additional Performance Metrics.....	31
Connection Sequence Metrics.....	31
Routing Metrics .....	32
General Fields .....	32
Session ISM Fields .....	36
RTSP Fields .....	36
Email Fields .....	36
FTP Fields.....	37
NNTP Fields .....	37
Glossary.....	38

## How to Use This Guide

This guide contains instructions on installing and using the PacketSight Information Source Module (ISM). It assumes a basic understanding of *XACCTusage*™ and its configuration and is intended to be used in conjunction with the *XACCTusage User Guide*.

## Document Conventions

The following typographic conventions are used in this guide:

Typeface or Symbol	Meaning	Example
<i>Italics</i>	References, new terms, and placeholders.	For a more detailed description of how PacketSight works, refer to Chapter 1 of the <i>XACCT PacketSight User Guide</i> .
<b>Bold</b>	Names of menus, options, and command buttons.	From the <b>Type</b> list, select <b>PacketSight</b> and then click <b>Next</b> .

## Contacting Technical Support

You can contact technical support by:

- Calling the number provided in your support agreement
- Sending an email to [support@xacct.com](mailto:support@xacct.com)
- Filling out the form available at <http://www.xacct.com> on the Web

When sending an email, please supply the following information:

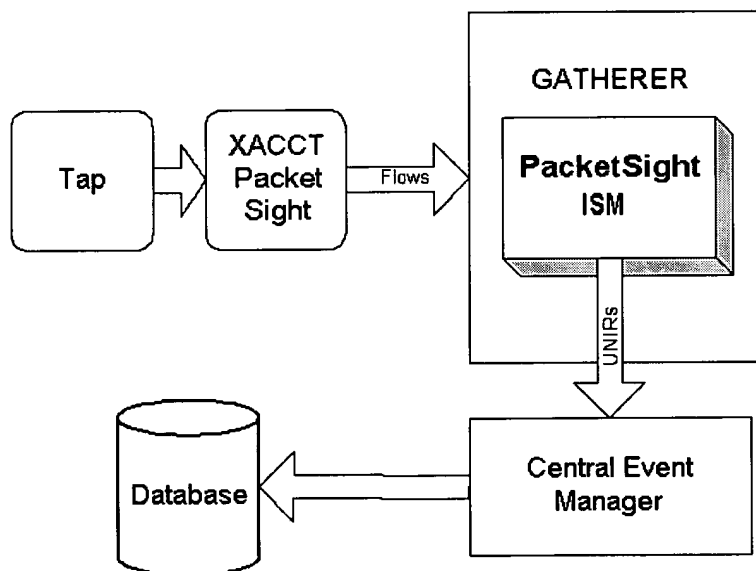
- Your name and the name of your company (your customer ID)
- Your contact information (telephone number and email)
- Product name and version number
- Problem description and any documentation that may help in resolving the problem
- Operating system, available RAM, database version, and memory usage on the machine on which the product is installed

## Overview

The PacketSight Information Source Module (ISM) is what *XACCTusage* uses to extract usage and QoS information from XACCT PacketSight. XACCT PacketSight retrieves information from network interface groups allowing you to collect statistical information about the traffic that passes through each interface. For additional information on XACCT PacketSight please refer to the *XACCT PacketSight User Guide*.

The PacketSight ISM is a Data Collection Module (DCM). The PacketSight ISM collects information, processes it, and relays it to its associated Gatherer for further enhancement and storage. It serves as the trigger for Enhancement Procedures and initiates the flow of data through *XACCTusage*.

The PacketSight ISM provides information for over 180 output fields. This enables you to track general information, such as Client and Server IP addresses, HTTP Response Time, and URL Domain names



*PacketSight ISM turning flows into UNIRs*

## Connecting With XACCTusage

The PacketSight ISM uses XACCT PacketSight as its Information Source. XACCT PacketSight reads packets from the network. The PacketSight ISM polls XACCT PacketSight in regular intervals to collect data. The PacketSight ISM converts the data into a Unified Network Information Record (UNIR). The UNIR is then pulled into XACCTusage by the Gatherer.

The Gatherer can then process and forward the UNIR to either of the following:

- Data Processing Module (DPM)
- Central Event Manager (CEM)

An example of a DPM is the Aggregator ISM. The Aggregator ISM reduces the amount of data flowing through the system by outputting only the most relevant information determined by you.

The data can also be enhanced by a Data Enhancement Module (DEM). An example of a DEM is the Session ISM. The Session ISM tags flows with identifiers (ID) to determine, among numerous other things, the duration of site visits.

## Features of the PacketSight ISM

This section summarizes some of the features of the PacketSight ISM.

**Note:** To start using the PacketSight ISM, you must install the software on the CEM host and then configure the ISM.

The PacketSight ISM provides you with these features:

- **Automated interface selection.** You do not have to add the interfaces from which you want the ISM to collect data when you configure the ISM. The ISM will monitor all the interfaces that are specified by XACCT PacketSight. This is convenient because it saves you the time and effort of adding interfaces manually. In addition to this, if new interfaces are added to the device, the ISM will automatically start monitoring them, eliminating the need for reconfiguring it.
- **A rich array of output fields.** The PacketSight ISM has many output fields allowing you to collect a rich array of data, including data such as **Client IP, URL Domain**, and many others. See the section “PacketSight ISM Output Fields” for a complete list.
- **Performance Metrics.** The PacketSight ISM enables the activation of specific Performance Metrics within the XACCT PacketSight Analyzer.
- **Event Handling.** The PacketSight ISM polls on pre-configured cycles for Events from the XACCT PacketSight Analyzer.
- **Data Enhancement.** The data polled is enhanced by adding timestamps, host domain exceptions, and more.

## Information Source Setup

XACCT PacketSight must be installed and reading from the network interface group. For instructions on how to install and configure XACCT PacketSight, please refer to the *XACCT PacketSight User Guide*.



## Installing the PacketSight ISM

You can install the PacketSight ISM on Sun Sparc systems running Solaris. You install the ISM on the Central Event Manager (CEM) host using the basic procedure for installing Information Source Modules.

To run the PacketSight Information Source Module (ISM) installation program, you need root user access rights for the host on which the Central Event Manager is installed.

To run the Module installation program

- 1 Log in as root user.
- 2 Copy the PacketSight.tar.Z file from the CD-ROM to your /tmp directory.
- 3 Enter `cd /tmp` to change to your tmp directory.
- 4 Extract the files from the compressed distribution file by executing the following command:

```
zcat PacketSight.tar.Z | tar xvf -
```

- 5 Execute the following command:

```
./xacct_upgrade
```

The XACCTusage installation program starts. The program runs automatically informing you of the actions performed and asking you to confirm and select options.

- 6 When prompted to read the End-user License Agreement, press Enter to display the text.
- 7 Read the End-user License Agreement.
- 8 Do one of the following:
  - Type `y` and press Enter, if you agree with the terms of the End-user License Agreement. The installation program proceeds to the next step.
  - Type `n` and press Enter, if you do not agree with the terms of the End-user License Agreement. The installation program shuts down.

If you accepted the terms of the End-user License Agreement, the list of components you can install displays.

=====

XACCTusage Module Installation

=====

You may choose components that will not be installed, by selecting their number or you can press c to continue, q to quit

Install	Name	Description
=====	====	=====
1 Yes	PacketSight	

Your selection :     c

**9** Select the components you want to install following the instructions on your screen. Use the following procedures to enter your selection.

- To change the installation status of a system component on the list (to alternate between Yes and No), type the number of the component and press Enter.
- To continue with installation, type c and press Enter. The components selected to be installed (marked with Yes) will be installed.
- To quit the installation program, type q and press Enter.

The selected components are installed. If installation is successful, the Central Event Manager sends the modules you have installed to the appropriate host or hosts. If installation is not successful, you get a notification with a description of the problem.

## Adding a PacketSight ISM to the XACCTusage Configuration

In order to use the PacketSight ISM, you must add an instance of it to the system configuration. You add the PacketSight ISM to its associated Gatherer.

To add the PacketSight ISM, you need the following:

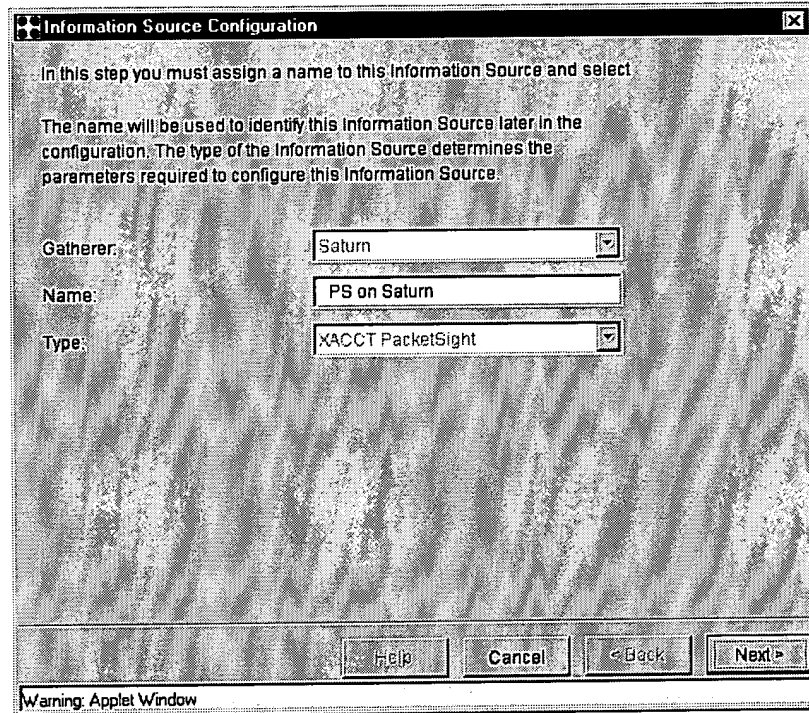
- Administrator or Manager access rights to the system.
- License to use the PacketSight Information Source Module installed. (See the section “Installing Licenses” in the *XACCTusage User Guide* for details.)
- The Gatherer that the PacketSight ISM will be associated with, configured in the system.

To add the PacketSight Information Source using the shortcut menu

- 1 In the *XACCTusage* tree, right-click the Gatherer to which you want to add the PacketSight Information Source, and then click **New Information Source**. The Information Source Configuration wizard is displayed.

## *Adding a PacketSight ISM to the XACCTusage Configuration*

- 2 In the **Name** box, type a unique name for this Information Source.



The dialog box is titled "Information Source Configuration". It contains the following text and fields:

In this step you must assign a name to this Information Source and select

The name will be used to identify this Information Source later in the configuration. The type of the Information Source determines the parameters required to configure this Information Source.

Gatherer: Saturn

Name: PS on Saturn

Type: XACCT PacketSight

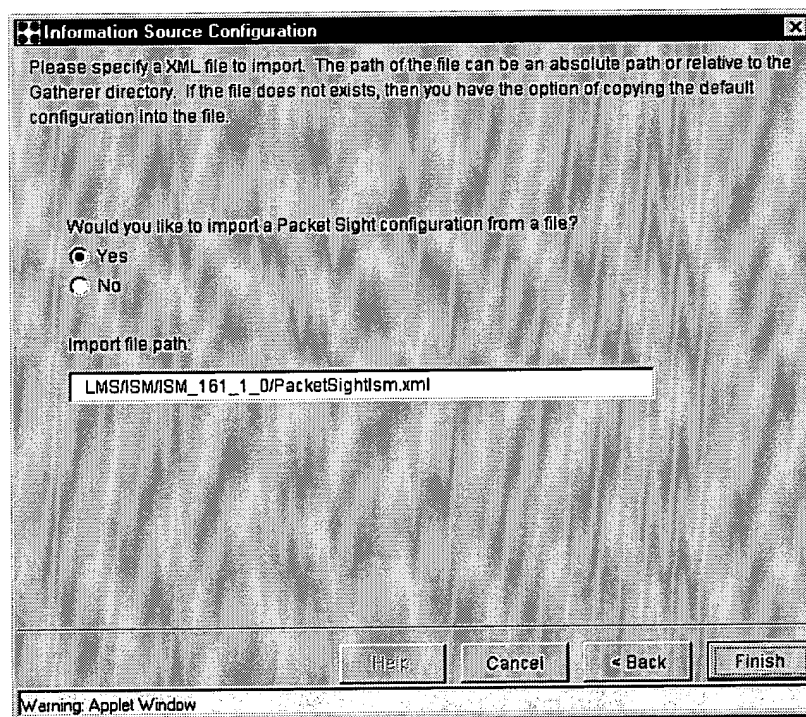
Buttons: Help, Cancel, < Back, Next >

Warning: Applet Window

- 3 From the **Type** list, select **XACCT PacketSight**.

- 4 Click **Next**. The next screen may take a minute or two to display as the ISM is now being downloaded to the Gatherer. This screen is used if you would like to import a configuration from a previous PacketSight ISM setup. To import the XML file, check the **Yes** button, and enter the path of the XML file containing the configuration information. Click **Finish** to import the file.

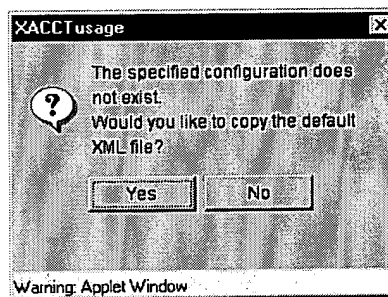
Click the **No** button if you do not have an XML configuration you would like to import, and would like to use the default configuration currently stored in the database. If there is no configuration stored in the database, the **No** button will be grayed out, and you will need to define the path of an XML file to import.



## Initial Setup

For the initial setup of the PacketSight ISM, the **No** button is grayed out. You can either enter a path containing an XML configuration, or click **Finish** without specifying a path.

When you click Finish without specifying a path, the following window appears:



Click **Yes** to accept the PacketSight ISM default XML configuration, or click **No** to return to the previous screen.

## Using XML to Configure the PacketSight ISM

The following two files are included with the PacketSight ISM and are used to configure the fields:

- **PacketSightIsM.dtd**: Defines the Document Type Definition (DTD) for the PacketSight configuration file.
- **PacketSightIsM.xml**: Contains the initialization configuration information of each field and points back to the PacketSightIsM.dtd file.

Once the PacketSightIsM.xml file is configured, you can use it to configure all other PacketSight ISMs on different Gatherers by importing the file. To configure the file you need a basic understanding of the eXtensible Markup Language (XML) and an XML editor. For more information about XML and DTD, please refer to one of the following sites:

<http://www.w3.org/XML>

<http://www.xml.org>

<http://www.xml101.com>

The tables on the following pages provide the parameters and switches for each of the elements.

## Data Collecting Elements

Elements	Description	Attributes	Default
<b>Probe ID</b>	Overrides default PROBE_ID.	Ranges from 0 to 4294967295 (Max INT32)	If 0, then Host ID
<b>LogConfig Verbosity</b>	Sets the log verbosity. The level of log information written to the log file.	<b>DEBUG:</b> outputs most information, slight reduction in performance. <b>INFO:</b> outputs ISM performance metric information to log file, slight reduction in performance. <b>ERROR:</b> outputs error messages only. No reduction in performance.	ERROR
<b>Log Config Path</b>	Sets file path for the log to be written.	Any valid file path on hard disk.	../Log/PacketSightIsm.log
<b>Regular Polling Interval</b>	Frequency in which all flows are to be pulled from the engine. The interval is synchronized to the hour and must divide evenly into 60.	1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, and 60 minutes	30 minutes
<b>EventPolling Interval</b>	Frequency specified event flows are extracted from the engine.	This value is synchronized to the hour, and must divide evenly into the RegularPollingInterval field.	60 seconds



## Event Elements

Event Elements configure the type of flows to pull from the engine during an event polling cycle. If not event is specified, then the Event polling is turned off, and the EventPollingInterval field is not used.

Elements	Description	Attributes
<b>StartEvent</b>	Gets only start flows out of the engine.	none
<b>DoneEvent</b>	Gets only done flows out of the engine.	none
<b>RangeEvent</b>	Gets flows out of the engine for range events.	<b>ARG:</b> Argument to which this range event applies (e.g. "BYTECNT" for "total byte count"). <b>OP:</b> The operator apply (e.g. "ARTHGT" for "arithmetic greater than"). <b>VALUE:</b> The value to compare against (e.g. "10000") The following argument will get flows with bytecounts greater than 10000: <RangeEvent ARG="BYTECNT" OP="ARTHGT" VALUE="10000"/>

## Domain Elements

The PacketSight ISM processed every HTTP Host request, and extracts the domain name based on the rules defined in RFC 1591 and other Internet RFCs. It takes into account the country code provided in the CountryCode file.

If the DomainException file exists, domain names in this file are not extracted and the full Host name is used. This allows you to distinguish between a specific list of domains to the rest of the domain names. This is used when you would like to have a break down of categories.

Examples of domain extraction:

www.xacct.com => xacct.com

travel.americanexpress => americanexpress.com

my.yahoo.com => yahoo.com

Example of a domain that will not be extracted if in the DomainException file:

travel.americanexpress.com => travel.americanexpress.com

Elements	Description	Attributes	Default
<b>Domain STATE</b>	Specifies how the PacketSight ISM should determine the Domain given a host name.	On or off. Setting this to "off " will disable the processing for the domain.	Off
<b>DomainException Interval</b>	Interval that the PacketSight ISM parses the DomainException.txt file		12 hours
<b>DomainExceptionFile</b>	Location of the domain exceptionfile.	Any valid file path on the hard disk	Path relative to the home directory of the XACCTusage Gatherer.
<b>CountryCodesFile</b>	File containing all of the Country Codes.	Any valid file path on the hard disk	Path relative to the home directory of the XACCTusage Gatherer.

## Probe Attributes

The following fields have been grouped together into logical blocks. This makes it easier to turn on and off entire groups of fields at one time. Turning a Group on/off will turn on/off all fields in that group. If the Group is “on”, then individual fields can be turned on/off by setting the **STATE** for that field (e.g. <Field NAME=”PS\_Timestamp\_Local” STATE=”off”/>).

Sample Groupings are **Timestamps** and **Service**. Descriptions of these fields can be found in the PacketSight ISM Output Fields section.

### Timestamps Group

Fields contained in the **Timestamps** Group.

- PS\_Timestamp\_Local
- PS\_Timestamp\_UTC
- PS\_Timestamp\_Begin
- PS\_Timestamp\_Update
- PS\_Timestamp\_End
- PS\_Time\_Zone\_Code
- PS\_Time\_Zone\_Bias\_From\_UTC
- PS\_Local\_Standard\_Time\_Zone
- PS\_Local\_DST\_Time\_Zone
- PS\_Day\_Light\_Saving\_Time\_Flag

### Services Group

Fields contained in the **Service** Group:

- PS\_Service\_Protocol
- PS\_Service\_R1
- PS\_Service\_R2
- PS\_Service\_R3
- PS\_Service\_R4
- PS\_Service\_R5
- PS\_Service\_R6
- PS\_Service\_R7
- PS\_Service\_R8
- PS\_Service\_R9
- PS\_Service\_R10
- PS\_Service\_R11
- PS\_Service\_R12

## Protocols

The Protocol elements specify for which protocols the PacketSight ISM should extract specific attributes. Supported Protocols are **HTTP**, **EMAIL**, **FTP**, **RTSP**, and **NNTP**. Unless otherwise specified, turning on/off a protocol will turn on/off all fields for that protocol. Each protocol contains a list of output fields/attributes associated with the protocol. Turning on individual fields for a given protocol will automatically specify the field to be an output field.

### HTTP Related Fields

- PS\_HTTP\_Domain
- PS\_HTTP\_Host
- PS\_HTTP\_Path
- PS\_HTTP\_Path\_Extension
- PS\_HTTP\_Response\_Code
- PS\_HTTP\_MIME\_Type
- PS\_HTTP\_MIME\_Subtype

### EMAIL Related Fields

- PS\_Email\_Incoming
- PS\_Email\_Outgoing
- PS\_Recipient\_Number

### FTP Related Fields

- PS\_Data\_User\_Name
- PS\_Anonymous\_Flag
- PS\_Filename
- PS\_Files\_Downloaded
- PS\_Files\_Uploaded

**RTSP Related Fields**

PS\_RTSP\_Domain  
PS\_RTSP\_Host  
PS\_RTSP\_Path  
PS\_RTSP\_Path\_Extension  
PS\_Media\_Player  
PS\_Media\_Type

**NNTP Related Fields**

PS\_Articles\_Posted  
PS\_Articles\_Read

## Configuring Performance Metrics

This section contains information for turning on/off different performance metrics in the the PacketSight core. For further information on Performance Metrics, please refer tot he *XACCT PacketSight User Guide*. The performance metrics are divided into the following:

- **PerformanceMetricCount:** metrics that only consist of a counter.
- **PerformanceMetricFull:** metrics with the full set of statistics (N, Min, Max, Sum X, Sum X2, and sum IX)

### Count Performance Metrics

The Count Performance Metric is a simple count that can be turned **on** or **off** by setting the STATE attribute (e.g. <PerformanceMetricCount NAME="PM\_CS\_ConnectionRetrans" STATE="on"/>). The following six metrics are Count Performance Metrics:

PM\_CS\_ConnectionRetrans  
PM\_SC\_ConnectionRetrans  
PM\_CS\_ConnectionOutOfOrders  
PM\_SC\_ConnectionOutOfOrders  
PM\_CS\_ConnectionClosedWindows  
PM\_SC\_ConnectionclosedWindows

## Full Performance Metrics

Each Full Performance Metric can have the following attributes:

- N** number of events (e.g., number of data packets)
- Min X** smallest value seen (e.g., smallest amount of data seen in a packet)
- Max X** largest value seen (e.g., largest amount of data seen in a packet)
- Sum X** sum of all values (e.g., total amount of data in all packets)
- Sum X2** sum of the squares of each value (computes standard deviation)
- Sum IX** sum of each sequence index (1,2, ...n) times its corresponding value

Each Full Performance Metric can be turned on or off. By default, all 6 Performance Metric attributes are off. Each Full Performance Metric can be turned on or off by setting the STATE attribute. The following metrics are Full Performance Metrics:

PM_ConnectionEstablishment	PM_CS_ART_ES
PM_ConnectionGracefulTermination	PM_CS_ART_SE
PM_ConnectionTimeoutTermination	PM_CS_ART_SS
PM_CS_ConnectionWindows	PM_SC_ART_ES
PM_SC_ConnectionWindows	PM_SC_ART_SE
PM_CS_Message_Jitter	PM_SC_ART_SS
PM_SC_Message_Jitter	PM_CS_ERT_ES
PM_CS_Stream_Jitter	PM_CS_ERT_SE
PM_SC_Stream_Jitter	PM_CS_ERT_SS
PM_CS_Hop_Count	PM_SC_ERT_ES
PM_SC_Hop_Count	PM_SC_ERT_SE
	PM_SC_ERT_SS

## PacketSight ISM Output Fields

The PacketSight ISM provide over 180 fields. This allows you to control which fields will be defined by the PacketSight ISM for future enhancement or insertion into the Database. They have been broken down into the following categories:

- Performance Metrics
- Additional Performance Metrics
- General Fields
- HTTP
- FTP
- RTSP
- NNTP
- POP3
- SMTP
- Email
- Session

### Performance Metrics

These fields all have the following six metrics:

- N** number of events (e.g., number of data packets)
- Min X** smallest value seen (e.g., smallest amount of data seen in a packet)
- Max X** largest value seen (e.g., largest amount of data seen in a packet)
- Sum X** sum of all values (e.g., total amount of data in all packets)
- Sum X2** sum of the squares of each value (computes standard deviation)
- Sum IX** sum of each sequence index (1,2, ...n) times its corresponding value



## Jitter Metrics

The Performance Metrics described in this section defines jitter as being the variance of the data packet observation time (e.g., the observed inter-data packet gap). It focuses solely on data arrival time. The Metric contains information about the Jitter (Inter-Packet Gaps) measured for data packets for a given application between two communicating end-points.

Field Name	Description
PS CS Msg Jitter	Measures the jitter for packets within data messages being exchanged from the <b>Client to Server</b> . Provides useful information about the performance of traffic in message-oriented (request/response) conversations. A data message starts with the first data packet from the client to the server and is demarcated (or terminated) by the first subsequent data packet in the other direction. Client to Server Inter-Packet Gaps are measured between data packets within the message.
PS SC Msg Jitter	Same as PS CS Msg Jitter, only <b>Server to Client</b> .
PS CS Strm Jitter	Measures the jitter for data packets being transferred from the <b>Client to the Server</b> . Client to Server Inter-Packet Gaps are measured between all data packets within the data stream. Provides useful information about the performance of traffic in conversations with independent, bi-directional data streams.
PS SC Strm Jitter	Same as PS CS Strm Jitter, only <b>Server to Client</b> .

## Exchange Response Metrics

Exchange Response Metrics consider the raw data streams of conversations when measuring response-time. They consider only the relative transfers of data packets without any further interpretation of the packets.

Exchange Response starts with the abstraction of a communicated exchange-message. An exchange-message is considered to start with a series of adjacent data packets transferred in a given direction (exchange message request). The end of such a message is defined to be the transfer of one or more adjacent data packets in the other direction (exchange message response).

The advantages of the Exchange Response set of metrics are that they:

- Can be applied uniformly to connectionless traffic
- Are very low in execution overhead to assess and detect.

Field Name	Description
PS CS ERT SS	<b>Client to Server Exchange Response Time Start to Start.</b> Measures the response time between the <b>start</b> of data messages from the Client to the Server and the <b>start</b> of their subsequent response data messages from the Server to the Client. A Client to Server data message starts with the first data packet from the Client to the Server and is demarcated (or terminated) by the first subsequent data packet in the other direction. The total time between the <b>start</b> of the Client to Server data message and the <b>start</b> of the Server to Client data message is measured with this metric.
PS CS ERT ES	<b>Client to Server Exchange Response Time End to Start.</b> Same as PS CS ERT SS, only End to Start.
PS CS ERT SE	<b>Client to Server Exchange Response Time Start to End.</b> Same as PS CS ERT SS, only Start to End.
PS SC ERT SS	<b>Server to Client Exchange Response Time Start to Start.</b> Measures the response time between the <b>start</b> of data messages from the Server to the Client and the <b>start</b> of their subsequent response data messages from the Client to the Server. A Server to Client data message starts with the first data packet from the Server to the Client and is demarcated (or terminated) by the first subsequent data packet in the other direction. The total time between the <b>start</b> of the Server to Client data message and the <b>start</b> of the Client to Server data message is measured with this metric.
PS SC ERT ES	<b>Server to Client Exchange Response Time End to Start.</b> Same as PS SC ERT SS, only End to Start.
PS SC ERT SE	<b>Server to Client Exchange Response Time Start to End.</b> Same as PS SC ERT SS, only Start to End.

## Application Response Metrics

Application Response Metrics build on the Exchange Response Metrics to consider the sequenced data streams of conversations when measuring response-time. They consider only the relative transfers of data packets that increase the sequence space for their direction of transfer.

Application Response starts with the abstraction of a communicated application-message. An application-message is considered to be a series of adjacent data packets transferred in a given direction and increasing the sequence space for that direction (application message request). The end of such a message is defined to be the transfer of one or more adjacent data packets increasing the sequence space in the other direction (application message response). Only initial (original) transmissions of data packets are considered within the scope of application response measurements.

The advantages of the Application Response set of metrics are:

- Can be applied uniformly to connection-oriented traffic.
- Modest execution overhead to assess and detect.
- These metrics try to avoid having to distinguish retransmissions from out-of-order packets. This is to avoid the concomitant overhead of duplicate detection within the scope of this metric.
- Are not skewed by retransmitted (duplicate) or out-of-order data packets.

Field Name	Description
<b>PS CS ART SS</b>	<p>Contains information about the Transport-level response time measured for message interactions of a given application between two communicating end-points. Measures the response time between the <b>start</b> of application messages from the <b>Client</b> to the <b>Server</b> and the <b>start</b> of their subsequent application message responses from the Server to the Client.</p> <p>A <b>Client to Server</b> application message starts with the first sequence-space increasing Transport Protocol Data Packet/Unit (TPDU) of a request from the <b>Client</b> to the <b>Server</b> and is demarcated (or terminated) by the first subsequent sequence-space increasing data packet of the response to the request. The total time between the <b>start</b> of the <b>Client</b> to the <b>Server</b> application message request and the <b>start</b> of the associated response from the Server to the Client is measured with this metric.</p>
<b>PS CS ART ES</b>	<b>Client to Server Application Response Time End to Start.</b> Same as PS CS ART SS, only <b>End to Start</b> .
<b>PS CS ART SE</b>	<b>Client to Server Application Response Time Start to End.</b> Same as PS CS ART SS, only <b>Start to End</b> .
<b>PS SC ART SS</b>	<p>Contains information about the Transport-level response time measured for message interactions of a given application between two communicating end-points. Measures the response time between the <b>start</b> of application messages from the <b>Server</b> to the <b>Client</b> and the <b>start</b> of their subsequent application message responses from the Client to the Server.</p> <p>A <b>Server to Client</b> application message starts with the first sequence-space increasing Transport Protocol Data Packet/Unit (TPDU) of a request from the <b>Server</b> to the <b>Client</b> and is demarcated (or terminated) by the first subsequent sequence-space increasing data packet of the response to the request. The total time between the <b>start</b> of the <b>Server</b> to the <b>Client</b> application message request and the <b>start</b> of the associated response from the Client to the Server is measured with this metric.</p>
<b>PS SC ART ES</b>	<b>Server to Client Application Response Time End to Start.</b> Same as PS SC ART SS, only <b>End to Start</b> .
<b>PS SC ART SE</b>	<b>Server to Client Application Response Time End to Start.</b> Same as PS SC ART SS, only <b>Start to End</b> .

## Connection Metrics

The PacketSight ISM supports Connection Metrics to report establishment and termination measures for conversations over reliable, connection-oriented Transport Protocols (e.g., TCP, SPX, etc.).

Field Name	Description
<b>PS Conn Establish</b>	<b>Connection Establishment:</b> Measures the number of connections established between end-points. Including: <ul style="list-style-type: none"> <li>• Number of transport connections successfully established</li> <li>• Set-up times of the established connections</li> <li>• Sum total of all the setup times for each connection.</li> <li>• Average setup time</li> </ul>
<b>PS Conn Graceful Term</b>	<b>Connection Graceful Termination:</b> Measures gracefully terminated connections both in volume and summary connection duration. Including: <ul style="list-style-type: none"> <li>• Number of gracefully terminated transport connections</li> <li>• Durations (lifetimes) of gracefully terminated connections</li> <li>• Sum of the total durations for all the connections</li> <li>• Average duration</li> </ul>
<b>PS Conn Timeout Term</b>	<b>Connection Timeout Termination:</b> Measures previously established and timed-out connections both in volume and summary connection duration. Including: <ul style="list-style-type: none"> <li>• Number of time-out transport connections</li> <li>• Durations (lifetimes) of timed-out terminated connections</li> <li>• Sum of the total durations for all the connections</li> <li>• Average duration</li> </ul>

## Connection Window Metrics

The PacketSight ISM supports Connection Sequence Metrics to report windowing performance measures for conversations over reliable, connection-oriented Transport Protocols (e.g. TCP, SPX, etc.).

Field Name	Description
<b>PS CS Conn Window</b>	<b>Client Server Connection Window:</b> Measures the number of transport-level packets containing windows from the <b>Client</b> to the <b>Server</b> and their relative window sizes. For some Transport Protocols the number of data packets may be estimated by taking the difference between the Window count of this metric and the overall traffic from the <b>Client</b> to the <b>Server</b> .
<b>PS SC Conn Window</b>	<b>Server Client Connection Window:</b> Same as PS CS Conn window, only <b>Server</b> to <b>Client</b> .
<b>PS CS Conn Closed Windows</b>	<b>Client Server Connection Closed Windows:</b> Measures number of Transport-level Windows from <b>Client</b> to <b>Server</b> within established connection lifetimes, which fully closed the acknowledge/sequence window.
<b>PS SC Conn Closed Windows</b>	<b>Server Client Connection Closed Windows:</b> Same as PS CS Conn closed Windows, only <b>Server</b> to <b>Client</b> .

## Additional Performance Metrics

### Connection Sequence Metrics

The PacketSight ISM supports Connection Sequence Metrics to report sequencing performance measures for conversations over reliable, connection-oriented Transport Protocols (e.g., TCP, SPX, etc.).

Field Name	Description
<b>PS CS Conn Retrans</b>	<b>Client Server Connection Retransmissions:</b> Measures number of actual events within established connection lifetimes in which transport, data-bearing packets from the Client to the Server were retransmitted.
<b>PS SC Conn Retrans</b>	<b>Server Client Connection Retransmissions:</b> Measures number of actual events within established connection lifetimes in which transport, data-bearing packets from the Server to the Client were retransmitted.
<b>PS CS Conn Out of Orders</b>	<b>Client Server Connection Out of Orders:</b> Measures the number of actual events within established connection lifetimes in which transport, data-bearing packets from the Client to the Server were detected as being out of sequential order.
<b>PS SC Conn Out of Orders</b>	<b>Server Client Connection Out of Orders:</b> Measures the number of actual events within established connection lifetimes in which transport, data-bearing packets from the Server to the Client were detected as being out of sequential order.



## Routing Metrics

The PacketSight ISM supports metrics to report routing performance measures for Network Layer protocols supporting routing information capabilities.

Field Name	Description
<b>PS CS Hop Count</b>	<b>Client Server Hop Count:</b> Measures the Hop Count (or routing distance measure) for Network-layer packets from the <b>Client</b> to the <b>Server</b> . Some network-layer protocols do not include routing distance values in their routing definitions. This metric will not be available or reported for traffic observed for such network-layer protocols.
<b>PS SC Hop Count</b>	<b>Server Client Hop Count:</b> Same as PS CS Hop Count only <b>Server</b> to <b>Client</b> .

## General Fields

Field Name	Description
<b>Event Type</b>	Type of flows to pull from the XACCT PacketSight engine during an event polling cycle. The different events are <b>Start</b> , <b>End</b> , and <b>Range</b> .
<b>Client IP Address</b>	The IP address that was assigned to the user for dialup of the permanent IP address for the client.
<b>Server IP Address</b>	IP address of server sending data.
<b>PS Src MAC Address</b>	Source MAC Address
<b>PS Dst MAC Address</b>	Destination MAC Address
<b>PS Probe ID</b>	Unique identifier for the probe that generated the data. Assigned by the Probe ID parameter in the XML file.
<b>PS Time Zone Bias From UTC</b>	The difference in seconds between the local time zone and the UTC (GMT) time zone.
<b>PS Day Light Saving Time Flag</b>	True, if it is day light savings time.
<b>PS Local Standard Time Zone</b>	Dependent upon the location of the PacketSight Analyzer.

Field Name	Description
<b>PS Local DST Time Zone</b>	Dependent upon the location of the PacketSight Analyzer.
<b>PS Time Zone Code</b>	Encodes the time zone information. (Offset from UTC in quarter-hours) * 2 + daylight-time flag. (e.g., EST (UTC – 5 hours, standard time) is $-5*2 = -10$ )
<b>PS Response Time</b>	Time between when the first HTTP request packet is sent and when the first response packet from the server is received.
<b>PS CS Response Time</b>	Client to Server Response time.
<b>PS SC Response Time</b>	Server to Client Response time.
<b>PS Service Protocol</b>	The network protocol of the flow (e.g. HTTP, TCP, and UDP)
<b>PS URL Host</b>	The hostname, if available, normalized to all lower-case.
<b>PS URL Path</b>	Entire path of the URL (e.g. www.xacct.com/careers/logo.gif would be /careers/logo.gif)
<b>PS URL Domain</b>	The domain (or site) derived from the hostname. (e.g. xacct.com)
<b>PS Begin Time</b>	Timestamp of the first packet seen in a flow. The value is the number of nanoseconds since January 1, 1970.
<b>PS Update Time</b>	Timestamp of the last packet seen in a flow. The value is the number of nanoseconds since January 1, 1970.
<b>PS End Time</b>	Timestamp of the last packet seen for the done flow. For TCP flows, it is the timestamp of the last observed flow, but it is possible for more flows due to time-outs or subflows. The value is the number of nanoseconds since January 1, 1970.
<b>PS Service R1 (R1-R12)</b>	Twelve separate fields. R1 is the first part on the right of Data_Service. Fields R12 is the twelfth part on the right of Data_Service. For example: <b>ether2.ip-v4.tcp.http.text.html</b> would be broken down as the following: R1=html R2=text R3=http R4=tcp R5=iv-v4 R6=ether2

Field Name	Description
PS MIME Type	Content type or media type of downloaded content. (e.g. text, image, application)
PS MIME Sub Type	Mime sub type (e.g. TIF, GIF, VPIM)
PS URL Path Extension	File extension of the URL. For example, <b>gif</b> would populate the field if the user went to <a href="http://www.xacct.com/careers/logo.gif">www.xacct.com/careers/logo.gif</a> .
PS Timestamp Local	Timestamp of the flow in local time.
PS Timestamp UTC	Timestamp of the flow in UTC (GMT) time.
PS Data User Name	Login name of the user for an FTP session.
PS Server Port	Server protocol port number (e.g. 80 for HTTP).
PS Client Port	Client protocol port number.
PS CS Connection Resets	Measures the Client to Server TCP connection resets.
PS SC Connection Resets	Measures the Server to Client TCP connection resets.
PS HTTP Response Code	Status code returned by web servers when a web page is requested.
PS Service	The name of the protocol (e.g. ether2).
PS CS Packets	Traffic packet count from client to server. Contains information about the volume of traffic measured for a given application between two communicating end points, from the client to server.
PS SC Packets	Traffic packet count from server to client. Contains information about the volume of traffic measured for a given application between two communicating end points, from the server to client.
PS CS Bytes	Volume of traffic measured for a given application between two communicating end points, from the client to the server. Indicates the byte count of traffic corresponding to the number of packets indicated by the PS CS Packets metric.
PS SC Bytes	Volume of traffic measured for a given application between two communicating end points, from the server to the client. Indicates the byte count of traffic corresponding to the number of packets indicated by the PS SC Packets metric.
PS Flow ID	A unique ID for a flow.

*PacketSight ISM Output Fields*

---

Field Name	Description
<b>PS Parent Flow ID</b>	A unique ID for a parent flow. Used for multiple flows in a session. (e.g., an http session starts multiple gifs download sessions)
<b>PS Aggregation Flag</b>	Only used internally with <i>XACCTusage</i> . It flags the field to specify whether or not it should be aggregated.

## Session ISM Fields

Use the following fields in conjunction with the Session ISM.

Field Name	Description
<b>PS Client Session</b>	Assigns Session IDs to Client Sessions.
<b>PS Server Session</b>	Assigns Session IDs to Server Sessions.
<b>PS Site Session</b>	Assigns Session IDs to Site Sessions.

## RTSP Fields

Field Name	Description
<b>PS Media Type</b>	Extracts Media Player URL.
<b>PS Media Player</b>	Establishes mapping for Media Player URL.
<b>PS Packets Dropped</b>	Number of packets dropped.

## Email Fields

Field Name	Description
<b>PS Email Incoming</b>	Number of incoming emails.
<b>PS Email Outgoing</b>	Number of outgoing emails.
<b>PS Recipient Number</b>	Number of recipients of email.

FTP Fields

Field Name	Description
<b>PS Files Uploaded</b>	Number of files uploaded.
<b>PS Files Downloaded</b>	Number of files downloaded.
<b>PS Filename</b>	Name of file uploaded or downloaded.
<b>PS Anonymous Flag</b>	This is true if the <b>PS Data Username</b> field is Anonymous.

NNTP Fields

Field Name	Description
<b>PS Articles Read</b>	Number of articles read.
<b>PS Articles Posted</b>	Number of articles posted.
<b>PS Newsgroup</b>	Name of Newsgroup.

## Glossary

**CEM:** See Central Event Manager.

**Central Event Manager (CEM):** A component of *XACCTusage* that coordinates, manages, and controls the operation of the system.

**Data Collection Module (DCM):** (Formerly called Asynchronous Information Source Module.) A type of Information Source Module that provides data from the network elements, for example, the Check Point FireWall-1 ISM.

**DCM:** See Data Collection Module.

**Data Enhancement Module (DEM):** (Formerly called Synchronous Information Source Module.) A type of Information Source Module that enhances the data gathered from the network elements, for example, the DNS ISM.

**DEM:** See Data Enhancement Module.

**Enhancement Procedure:** The set of operations that define the route of the network session record from the Information Source that supplies the initial data (the trigger of the Enhancement Procedure) to the place where the data is stored (the target). The Enhancement Procedure includes Field Enhancements on every field of the target that receives information originating from the trigger.

**Field Enhancement:** Part of an Enhancement Procedure that defines how the data obtained from its trigger is used to fill a single field in the target.

**Gatherer:** A component of *XACCTusage* whose main function is to collect network traffic data from the Information Sources located on the network. The Gatherers defined are multi-threaded lightweight smart-agents designed to run on non-dedicated hosts as background processes.

**Information Source (IS):** 1. A network device or application server from which *XACCTusage* collects network session data. An Information Source can be a mail server, a firewall, a router, a DNS server, and the like. 2. An instance of an Information Source Module that is part of the *XACCTusage* configuration and hence is a system configuration object. For example, an Information Source of type DNS, called **dns-xacct**, which is part of the *XACCTusage* configuration and appears as an object in the XACCT tree.

**Information Source Module (ISM):** An add-on to *XACCTusage* whose function is to provide an interface between a Gatherer and a specific network element.

**IP address:** Internet Protocol address. A 4-byte address that uses numbers (rather than names) and uniquely identifies a host computer on the Internet, for example, **200.201.32.1**. The IP address can be split into a network number (or network address), a host number (a number unique to each host on the network), and sometimes also a sub-net mask.

**IS:** See Information Source.

**ISM:** See Information Source Module.

**Unified Network Information Record (UNIR):** A compact and efficient generic format in which network data is maintained and processed in *XACCTusage*.